Question 1

1. Define what it means for $< G, * >$ to be a group.

   Solution: A group $< G, * >$ consists of a set G together with a binary operation $* : G \times G \to G$ that satisfies:

   (a) G contains an identity, *i.e.* there exists $e \in G$ such that, for all $g \in G$

   $$g * e = e * g = g.$$

   (b) G contains inverses, *i.e.* for all $g \in G$ there exists $h \in G$ such that

   $$g * h = h * g = e.$$

   (c) The operation $*$ is associative, *i.e.* for all $g, h, k \in G$

   $$(g * h) * k = g * (h * k).$$

2. Define what it means for a map $\varphi : S \to T$ to be an isomorphism of groups $< S, * >$ and $< T, \star >$.

   Solution: The map $\varphi : S \to T$ must be a bijection and must satisfy the homomorphism property, *i.e.* for all $g, h \in G$

   $$\varphi(g * h) = \varphi(g) \star \varphi(h).$$

3. Complete the following table to make it a group

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

4. Is $< \mathbb{R}, \times >$, the real numbers with the usual multiplication, a group ? Justify your answer.

   Solution: $\mathbb{R}$ with the usual operation of multiplication is not a group since $0 \in \mathbb{R}$ has no inverse.

Question 2

1. Define what it means for $x \in S$ to be an identity element for the binary structure $< S, * >$.

   Solution: An element $x \in S$ is an identity element for $< S, * >$ if for all $s \in S$,
$$s * x = x * s = s.$$

2. Prove that an identity element of a binary structure, if it exists, is unique.

   Solution: Let $< S, * >$ be a binary structure. Suppose that $e_1, e_2 \in S$ are identity elements. Then
$$\begin{aligned} e_1 &= e_1 * e_2 && \text{since } e_2 \text{ is an identity} \\ &= e_2 && \text{since } e_1 \text{ is an identity} \end{aligned}$$

3. Suppose $e \in S$ is an identity element for $< S, * >$. Suppose $\varphi : S \to T$ is an isomorphism of binary structures $< S, * >$ and $< T, \star >$. Show that $< T, \star >$ has an identity element.

   Solution: Let $t \in T$ be arbitrary. Define e_S be the (unique) identity element in S. Define $e_T = \varphi(e_S)$. Since φ is a bijection there exists $s \in S$ such that $\varphi(s) = t$. Now
$$\begin{aligned} t \star e_T &= \varphi(s) \star \varphi(e_S) && \text{definition} \\ &= \varphi(s * e_S) && \text{homomorphism property} \\ &= \varphi(s) && e_S \text{ is the identity} \\ &= t && \text{definition.} \end{aligned}$$

   Similarly
$$\begin{aligned} e_T \star t &= \varphi(e_S) \star \varphi(s) && \text{definition} \\ &= \varphi(e_S * s) && \text{homomorphism property} \\ &= \varphi(s) && e_S \text{ is the identity} \\ &= t && \text{definition.} \end{aligned}$$

   Thus
$$e_T \star t = t \star e_T = t.$$

   Since $t \in T$ was arbitrary this hold for all $t \in T$ and we have e_T is an identity element in T.

Question 3

1. Let $\varphi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$. Suppose $\varphi(2) = 5$. Can φ be an automorphism of $< Z_{10}, +_{10} >$? Justify your answer.

   Solution: No. Several possible arguments.

   An isomorphism prerves the order of an element thus no isomorphism can take 2, which is order 5, to 5, which is order 2.

   Assume φ has the homomorphism property. Then

   $$\varphi(4) = \varphi(2 +_{10} 2) = \varphi(2) +_{10} \varphi(2) = 5 +_{10} 5 = 0$$

   but $\varphi(0) = 0$ thus *varphi* is not a bijection.

   Assume φ has the homomorphism property. Then $\varphi(2) = \varphi(1) +_{10} \varphi(1)$ which must be even. This contradicts $\varphi(2) = 5$.

2. Determine the number of automorphisms of $< \mathbb{Z}_{10}, +_{10} >$.

   Solution: We know that an automorphism preserves the order or an element and hence takes generators to generators. There are 4 generators for $< \mathbb{Z}_{10}, +_{10} >$; 1, 3, 7, and 9. Thus there are 4 possible automorphisms generated by $\varphi(1) = 1$, $\varphi(1) = 3$, $\varphi(1) = 7$, and $\varphi(1) = 9$ respectively.

3. Let $\varphi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ be an automorphism of $< \mathbb{Z}_{10}, +_{10} >$ with $\varphi(7) = 1$. Find $\varphi(1)$. Justify your answer.

   Solution: Either check the four above or directly compute

   $$\varphi(1) = \varphi(7 +_{10} 7 +_{10} 7) = \varphi(7) +_{10} \varphi(7) +_{10} \varphi(7) = 1 +_{10} 1 +_{10} 1 = 3.$$

   Thus $\varphi(1) = 3$.

4. Determine the number of automorphisms of $< \mathbb{Z}, + >$.

   Solution: There are only two generators for $< \mathbb{Z}, + >$; 1 and -1. Thus there are two automorphisms, generated by $\varphi(1) = 1$ and $\varphi(1) = -1$. The first is the identity, $\varphi(x) = x$, and the second is $\varphi(x) = -x$.

Question 4

1. Define the order of an element $x \in G$ of a group $< G, * >$.

   Solution: The order of an element x can be described in two equivalent ways:

   (a) the smallest number positive integer n such that $x^n = e$.

   (b) the cardinality of the cyclic group generated by x.

2. Determine the order of the element $525 \in \mathbb{Z}_{3465}$. Hint: $3465 = 3^2 \times 5 \times 7 \times 11$ and $525 = 3 \times 5^2 \times 7$.

   Solution: We have $\gcd(525, 3465) = 3 \times 5 \times 7 = 105$. Thus $< 525 >=< 105 >$ and the order of this group is

$$\frac{3465}{105} = 3 \times 11 = 33.$$

3. Find all the subgroups of Z_{84} and draw the subgroup diagram. Hint: $84 = 2^2 \times 3 \times 7$

   Solution: